REMARKS

Claims 1-21 and 24-28 were presented for examination and were pending in this application. In the Office Action dated August 14, 2008, claims 1-21 and 24-28 were rejected. Applicant thanks the Examiner for examination of the claims pending in this application and addresses the Examiner's comments below. Based on the above Amendment and the following Remarks, Applicant respectfully requests that the Examiner reconsider all outstanding objections and rejections, and withdraw them.

35 U.S.C. § 103 Rejection

Claims 1-3, 6, 8-11, 14, 16-18, 21, and 24-28 stand rejected under 35 U.S.C. §103 as being unpatentable over Pisello et al. (U.S. Patent No. 5,495,607) in view of Stupek et al. (U.S. Patent No. 5,586,304), and in further view of Schmidt et al. (U.S. Patent No. 6,535, 894). Claims 4, 12, and 19 stand rejected under §103 as being unpatentable over Pisello in view of Stupek, in further view of Schmidt, and in further view of Fischer (U.S. Patent No. 5,694,569). Claims 5, 13, and 20 stand rejected under §103 as being unpatentable over Pisello in view of Stupek, in further view of Schmidt, and in further view of Baker (U.S. Publication No. 2003/0233352). Claims 7, 15, and 22 stand rejected under §103 as being unpatentable over Pisello in view of Stupek, in further view of Schmidt, and in further view of Chino (U.S. Publication No. 2002/0046207). Applicant now traverses these rejections.

Claim 1 as amended recites *inter alia*:

> retrieving from the plurality of records in the database a first record associated with the examined one of the plurality of files;
> retrieving from the plurality of records in the database a second record associated with a malicious file;
> analyzing the gleaned file attributes gleaned from the examined one of the plurality of files, the gleaned file attributes having been retrieved from the first record;

> analyzing one or more attributes of the malicious file, the one or more attributes of the malicious file having been gleaned from the second record; and
> determining whether a status of the examined one of the plurality of files is malicious, responsive to analyzing the gleaned file attributes and the one or more attributes of the malicious file.

The claimed invention thus relates to analyzing attributes gleaned from a first file and a malicious file in order to determine whether the first file is malicious.

None of Pisello, Stupek, and Schmidt disclose "retrieving from the plurality of records in the database a second record associated with a malicious file" or "analyzing one or more attributes of the malicious file, the one or more attributes of the malicious file having been gleaned from the second record" or "determining whether a status of the examined one of the plurality of files is malicious, responsive to analyzing the gleaned file attributes and the one or more attributes of the malicious file."

Pisello discloses a network management system that has a virtual catalog overview of files distributed across a network domain, used to assist in "auditing or locating files located anywhere in the domain" and "for transferring files across the domain." Pisello, Abstract. Pisello, however, does not disclose "retrieving from the plurality of records in the database a second record associated with a malicious file" or "analyzing one or more attributes of the malicious file, the one or more attributes of the malicious file having been gleaned from the second record" or "determining whether a status of the examined one of the plurality of files is malicious, responsive to analyzing the gleaned file attributes and the one or more attributes of the malicious file."

Stupek does not remedy the above-stated deficiencies of Pisello. Stupek discloses a "method for use in upgrading a resource of a computer from an existing version of the resource to a later version of the resource" including storing the existing version, the later version number, and the differences between the versions, and comparing the respective

version numbers. Stupek, Abstract. However, Stupek does not disclose "retrieving from the plurality of records in the database a second record associated with a malicious file" or "analyzing one or more attributes of the malicious file, the one or more attributes of the malicious file having been gleaned from the second record" or "determining whether a status of the examined one of the plurality of files is malicious, responsive to analyzing the gleaned file attributes and the one or more attributes of the malicious file."

Schmidt does not remedy the above-stated deficiencies of Pisello and Stupek. Schmidt discloses a method of incremental updating of archive files by transmitting to a target the difference file containing the differences between the original source file and the updated source file; the target applies the received differences. Schmidt, Abstract.

To ensure that the difference file is not deliberately corrupted, Schmidt uses digital signatures. The source digitally signs the difference file and the target verifies the authenticity of difference file by comparing the received sign with the source's digital sign. Schmidt, col. 9, ll. 43-64. Schmidt signs a difference file at the *source site*, thus is it not malicious. When received at the destination site, the difference file is compared using the digital signature associated with the difference file. Thus, the destination site compares the known difference file signature with the difference file. Schmidt does not disclose comparison to a malicious file. Schmidt therefore does not disclose analyzing the attributes of a malicious file and determining if a file is malicious in response to the analysis of the malicious file's attributes.

Indeed, Schmidt teaches away from a modification including analyzing the attributes of a malicious file and determining if a file is malicious in response to the analysis of the malicious file's attributes. In Schmidt, analyzing the attributes of a malicious file would be counterproductive because the attributes of a malicious file are not

helpful in ensuring that the received file is from a trusted source. Schmidt uses the digital signature of the trusted site, and not the attributes of a malicious file, to verify that the received file is from a trusted source. Analyzing the attributes of a malicious file in Schmidt will consume processing power, slow down the verification process, and achieve nothing. Schmidt therefore teaches away from analyzing the attributes of a malicious file and determining if a file is malicious in response to the analysis of the malicious file's attributes.

Thus, Schmidt also does not disclose "retrieving from the plurality of records in the database a second record associated with a malicious file" or "analyzing one or more attributes of the malicious file, the one or more attributes of the malicious file having been gleaned from the second record" or "determining whether a status of the examined one of the plurality of files is malicious, responsive to analyzing the gleaned file attributes and the one or more attributes of the malicious file."

Thus, the deficient disclosures of these references, considered either alone or in the combination suggested by the Examiner, fail to establish even a *prima facie* basis from which a proper determination of obviousness under 35 U.S.C. § 103(a) can be made. A *prima facie* showing of obviousness requires that the reference(s) teach or suggest all the claim limitations. As discussed above, the references do not teach or suggest all of the claimed limitations. Claim 1 is therefore patentable over Pisello, Stupek, and Schmidt, alone or in the suggested combination.

Independent claims 9 and 16 are patentable over Pisello, Stupek, and Schmidt, alone or in the suggested combination, for the above-stated reasons. Claims 2-8 and 24-28 depend from claim 1. Claims 10-15 depend from claim 9 and claims 17-21 depend from claim 16. These dependent claims include all the above mentioned limitations of their

independent claims. Pisello, Stupek and Schmidt, alone and in combination, do not disclose the above mentioned limitations. In addition, these claims recite other patentably distinguishable features not included in their respective base claims. Thus, these claims are patentable over Pisello, Stupek, and Schmidt, alone and in combination, for at least these reasons.

With respect to dependent claims 4, 5, 7, 12, 13, 15, 19, 20, and 22, Fischer, Baker, and/or Chino, alone or in the suggested combinations, also do not remedy the above-discussed limitations, nor does the Examiner alleged that they do. Rather, Fischer, Baker, and/or Chino are cited for features in dependent claims 4, 5, 7, 12, 13, 15, 19, 20, and 22. Thus, dependent claims 4, 5, 7, 12, 13, 15, 19, 20, and 22 also are patentable over Fischer, Baker, and Chino, alone or in the suggested combinations.

Conclusion

In sum, Applicant respectfully submits that claims 1-21 and 24-28, as presented herein, are patentably distinguishable over the cited references. Therefore, Applicant requests reconsideration of the basis for the rejections to these claims and requests allowance of them. In addition, Applicant respectfully invites the Examiner to contact Applicant's representative at the number provided below if the Examiner believes it will help expedite furtherance of this application.

Respectfully submitted,
WILLIAM E. SOBEL

Dated: November 13, 2008

By: /Jennifer R. Bush/
Jennifer R. Bush, Reg. No. 50,784
Attorney for Applicants
Fenwick & West LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
Tel.: (650) 335-7213
Fax: (650) 938-5200

20423/08016/DOCS/1985701.4